Design Principles for Robust ISHM

Integrated Systems Health Management (ISHM) will be a critical element for Exploration mission vehicles and systems. To provide reliable and robust results, we assert that ISHM systems *must* be integrated with functional design of the systems they will be used for. A significant challenge is the lack of formal design methods and tools to enable this integration. We propose to leverage existing formal design practices and methodologies for functional/conceptual design so that ISHM design can be seamlessly incorporated into system and design work practices.

Background

Integrated Systems Health Management (ISHM) *must* be integrated into new systems starting with the early design stages. ISHM is a systems engineering discipline that promises significant benefits in **safety, reliability, and affordability**. Despite significant improvements in health management solutions, simply retrofitting ISHM systems into existing systems is not effective. Last-minute retrofits result in unreliable systems, ineffective solutions, and excessive costs (e.g., Space Shuttle TPS monitoring which was considered only after 110 flights and the Columbia disaster). High false alarm or false negative rates due to substandard implementations hurt the credibility of the ISHM discipline.

There are several challenges to widespread ISHM implementation and use today. These include:

•Lack of tools and processes for integrating ISHM into the vehicle system/subsystem design;

•Standards and interfaces with limited following (e.g., Open System Architecture for Condition Based Maintenance (OSACBM));

•Limited appreciation for ISHM in engineering design practice.

In our work, we assert that ISHM systems *must* be integrated with new systems starting from the early design stages. Tools and processes for integrating ISHM into the vehicle system/subsystem design are currently nonexistent. The objective of the proposed effort is to demonstrate the integration and use of system/subsystem design, analysis and diagnostic tools/models in the design and implementation of both real-time onboard and ground-based ISHM. We will leverage existing formal design practices and methodologies for functional/conceptual design so that design for health maintenance can be seamlessly incorporated into system and design engineer work practices.

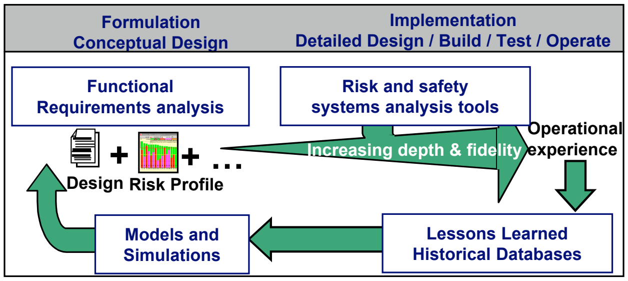

Figure 1: Risk analysis during the product lifecycle.

Research Overview

We focus on early design stages because studies and design reviews have shown that this early stage presents the best opportunity to catch potential failures and anomalies. Decisions such as sensor selection, measurement points, modeling, model-checking, diagnosis, and signature and data fusion, risk analysis, and software reliability, need to be made early in design, with the design team directly in the loop. In addition, hardware and software architecture, interfaces and standards will be developed for ISHM systems.

NASA currently employs a number of risk analysis tools and methods, including FMEA, FTA and PRA, and design engineers have used them successfully for designing reliable and safe systems. But these methods have drawbacks that limit their applicability to design for ISHM. We will begin by surveying current Risk Analysis methods and tools at NASA to determine which are most applicable to design for ISHM. Next, we will extend those methods to suit design for ISHM goals. We have already begun work in developing failure analysis methods that determine failures modes during the early stage of functional design.

Design Principles and formal methods for Robust ISHM

An example of formal design methods is risk analysis to optimize the benefits of integrating ISHM into a system design. Applied haphazardly, ISHM may provide benefits but also add significant costs to a system. Risk analysis can be applied at two levels. In the first level, risk analysis identifies and prioritizes system risks and then points out those risks where ISHM technologies can be applied to mitigate those risks. Secondly, risk analysis can be used to study the space of system designs with IVHM integration and to aid in decision-making for when to apply ISHM. We plan to apply risk analysis to optimize the use of the ISHM system to find the best balance between cost, performance, safety and reliability throughout the lifecycle (Figure 1). In our work, we will incorporate risk analysis into a “design for ISHM” design methodology and develop risk analysis tools to support the methodology.

Another example of a formal approach is function-based failure identification. Previous work on elemental function-failure design has shown how failure analysis can be applied during the conceptual design, before any physical design choices have been made (Figure 2). We plan to extend this method for application to ISHM design, incorporating results from research on intelligent sensor selection and placement. Computer tools for supporting these design methods will be incorporated into our integrated ISHM design environment.

In this research element, we are working on ISHM specific risk and failure modes analysis tools with the following characteristics:

-Can be used during early phases of design when ISHM design decisions can have the largest impact;

-Characterizes the risks for which ISHM technologies provide the best mitigation;

-Aids engineers in understanding the value of ISHM in system design;

-Allows functional design team to determine the types of failures we can expect.

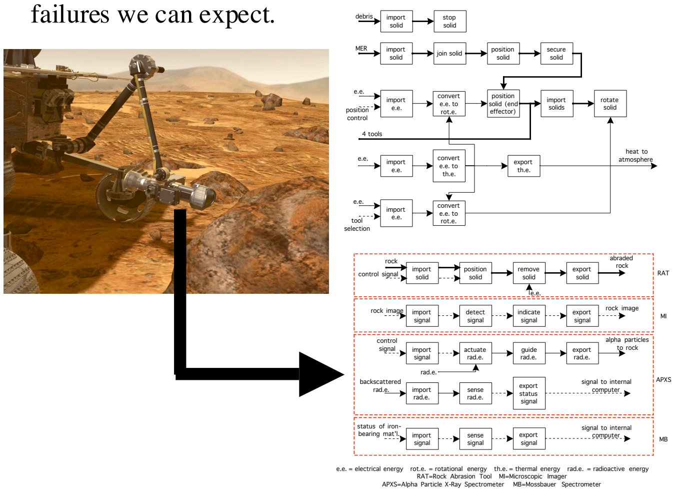

Figure 2: Function-based failure prevention in design.

These specialized ISHM risk analysis tools are to be integrated into our ISHM design environment. Our specialized risk analysis tools will streamline the design process by making it possible for design engineers to make decisions about when and how to incorporate ISHM into a design without consulting ISHM experts.

Subsequent phases will extend the work to address a greater segment of the vehicle system/ISHM hierarchy and focus on crewed spacecraft. An ARC-based design simulation environment will be the end capability. Throughout this effort, we will adopt and use existing and emerging standards such as OSACBM.

Relevance to Exploration Systems

NASA’s new exploration theme poses stringent demands on vehicles and systems that will be relied upon for day-to-day operations in space. ISHM will be a critical capability required for all **space, lunar, and planetary exploration vehicles and systems**, including transportation systems and robotic systems. Fundamental ISHM roles include **automated spacecraft and vehicle health self-assessment, on-demand vehicle maintenance scheduling, and crew emergency response advisory**. Monitoring and management of the health state of diverse components, subsystems, and systems is a difficult task, and will only become more challenging when required and implemented for long-term and evolving missions. The design for ISHM environment envisioned here will enable a robust **system-of-systems level** capability. The result will be designs for robust ISHM systems with an overall impact of reducing operations cost, increasing safety and reliability, sustaining engineering activities.

H&RT Program Elements:

This research capability supports the following H&RT program /elements:

ASTP/Advanced Studies, Concepts & Tools/ Software, Intelligent Systems & Modeling

Points of Contact:

Dr. Irem Y. Tumer
650-604-2976, itumer@mail.arc.nasa.gov
http://ic.arc.nasa.gov/~itumer
Dr. Francesca Barrientos
650-604-2976, fbarrientos@mail.arc.nasa.gov
Dr. Serdar Uckun
650-604-4996, uckun@mail.arc.nasa.gov